Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP05/054004

International filing date: 15 August 2005 (15.08.2005)

Document type: Certified copy of priority document

Document details: Country/Office: DE
Number: 10 2004 039 899.2
Filing date: 17 August 2004 (17.08.2004)

Date of receipt at the International Bureau: 15 September 2005 (15.09.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	10 2004 039 899.2
Anmeldetag:	17. August 2004
Anmelder/Inhaber:	Dr. Katharina S c h e j a , 65812 Bad Soden/DE; Professor Dr.-Ing. Dmitri K o r o b k o v, 60322 Frankfurt am Main/DE
Bezeichnung:	Verschlüsselungsverfahren
IPC:	H 04 L 9/22

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 8. August 2005
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Stenk

A 9161
03/00
EDV-L

Anmelder:
Dr. Katharina Scheja
Eifelstraße 3
65812 Bad Soden

Prof. Dr.-Ing. Dmitri Korobkov
Leerbachstraße 50
60322 Frankfurt

Verschlüsselungsverfahren

Beschreibung

Die Erfindung betrifft eine Vorrichtung und ein Verfahren zur Verschlüsselung einer digitalen Kommunikation. Insbesondere betrifft die Erfindung ein Verfahren zur Bereitstellung von Schlüsseln in einem symmetrischen Verschlüsselungsverfahren.

Gebiet der Erfindung:

Nach Shannon [1,2] lässt sich die Sicherheit eines Verschlüsselungssystems darstellen als bedingte Entropie der unverschlüsselten Datenfolge, bei bekannter verschlüsselter Datenfolge.

Die bedingte Entropie kann höchstens so groß sein wie die Länge der zufälligen Schlüsselfolge (Crypto Sequenz) [3].

Als Folge ist die theoretisch vollkommene Verschlüsselung nur dann zu erreichen, wenn die Schlüsselfolge mindestens so groß ist wie die Datenfolge.

Hierbei ist die Crypto Sequenz zufällig mit gleichwahrscheinlichen Symbolen und hat die gleiche Länge wie die Datenfolge (Plain Text). Jede Crypto Sequenz wird nur ein einziges Mal verwendet (One Time Pad).

Der Nachteil an diesem Ansatz ist, dass die vollkommene Verschlüsselung eine sehr lange Schlüsselfolge erfordert.

In der Praxis wird bislang eine pseudozufällige Crypto Sequenz mit einem Verschlüsselungsautomaten (Cypher) generiert. Zur Erzeugung der pseudozufälligen Crypto Sequenz werden Anfangszustand des Verschlüsselungsautomaten und eine Schlüsselfolge benötigt. Anfangszustand und Schlüsselfolge müssen sowohl beim Verschlüsseln als auch beim Entschlüsseln bekannt sein. In der Regel ist die Schlüsselfolge viel kürzer als die daraus generierte pseudozufällige Crypto Sequenz.

Überblick über die Erfindung:

Aufgabe der vorliegenden Erfindung ist es, ein Verfahren und eine Vorrichtung bereitzustellen, die bei einer Kommunikation, wie einer mobilen Kommunikation, eine möglichst optimale Verschlüsselung ermöglicht.

Diese Aufgabe wird durch die Erfindungen mit den Merkmalen der unabhängigen Ansprüche gelöst. Vorteilhafte Weiterbildungen der Erfindungen sind in den Unteransprüchen gekennzeichnet.

Im erfindungsgemäßen Verfahren wird die zufällige Crypto Sequenz nicht in einem Verschlüsselungsautomaten erzeugt, sondern aus einem Vorrat gleichwahrscheinlicher Symbole entnommen, die vorzugsweise in einem FLASH-EPROM abgelegt wurden oder auch auf einer FLASH-CARD bzw. einem FLASH-Speicher abgelegt sind. Andere kleine Speichermodule, die

unempfindlich sind und in portablen Kommunikationsgeräten eingesetzt werden können, sind ebenfalls denkbar, wie Minidisks oder sehr kleine Festplatten. Holografische Speicher oder Nanospeicherelemente sind ebenfalls denkbar, soweit sie mobil eingesetzt werden können. Da es sich um ein symmetrisches Verfahren handelt, sollte der Inhalt des FLASH-EPROM für Verschlüsselung und Entschlüsselung identisch sein. Somit werden für die Kommunikation zweier Geräte zwei Kopien des FLASH-EPROMs angelegt. Sollten noch mehr Teilnehmer an der Kommunikation teilnehmen (z. B. Polizeifunk), so sind entsprechend viele Kopien bereitzustellen.

Der Vorrat an entnommener zufälliger Crypto Sequenz vom Speichermedium hat die gleiche Länge wie die zu verschlüsselnde Datenfolge. Damit wird die theoretisch vollkommene Verschlüsselung nach Shannon erreicht.

Für die Ver- und Entschlüsselung sollte die Anfangsadresse der entnommenen Crypto Sequenz bekannt sein.

Beim Stand der Technik und somit in konventionellen Verfahren erfolgt eine Synchronisation der Ver- und Entschlüsselung durch Übertragung des Anfangszustandes des Verschlüsselungsautomaten (Cyphers).

Im erfindungsgemäßen Verfahren, das z. B. Zugriff auf einen großen FLASH-Speicher hat, wird zur Synchronisation die Anfangsadresse der Leseoperation mit übertragen.

Bei sequentieller Abarbeitung des FLASH-Inhaltes kennzeichnet die Anfangsadresse die Grenze zwischen verbrauchter und unverbrauchter Crypto Sequenz

In einer weiteren Ausführungsform kann anstelle eines sequentiellen Auslesens des FLASH-Inhaltes ein Auslesen an pseudozufälligen Adressen durchgeführt werden. Die pseudozufälligen Adressen werden in einem

Pseudozufallsgenerator (PZG) anhand eines Anfangszustandes und eines Schlüssels erzeugt. Eine Mehrfachnutzung des FLASH-Inhaltes wird ermöglicht, kann jedoch im Einzelfall auch vermieden werden.

Zur Synchronisation der Ver- und Entschlüsselung wird in der weiteren Ausführungsform des Verfahrens der Anfangszustand des Pseudozufallsgenerator (PZG) mit übertragen.

In einer weiteren Ausführungsform, dem so genannten „Fire and Forget"-Verfahren, wird eine Information in Blöcken übermittelt, ohne ein Gedächtnis an vorausgegangene Blöcke.

Der Empfänger muss anhand eines einzigen empfangenen Blockes in der Lage sein, zu synchronisieren und die Information zu rekonstruieren.

Im konventionellen Verfahren muss hierbei in jedem Block in einer Präambel der Zustand des Cyphers mit übertragen werden. In der Regel ist die hierzu benötigte Redundanz sehr hoch.

Im erfindungsgemäßen Verfahren wird in jedem Block in einer Präambel der Zustand des Pseudozufallsgenerators mit übertragen. In der Regel ist die hierzu benötigte Redundanz wesentlich geringer.

In noch einer weiteren Ausführungsform kann anstelle eines sequentiellen Auslesens des FLASH-Inhaltes ein Auslesen an pseudozufälligen Adressen durchgeführt werden. Die pseudozufälligen Adressen werden in einem Pseudozufallsgenerator (PZG) anhand eines Anfangszustandes und eines Schlüssels erzeugt. Eine Mehrfachnutzung des FLASH-Inhaltes wird ermöglicht.

Zur Synchronisation wird hierbei anstatt der Adresse der Zustand des PZGs übertragen.

In einer weiteren alternativen Ausführungsform wird zusätzlich eine Permutation der Daten vorgenommen, um die Positionen der Synchroninformation (Zustand des PZG) zu verstecken.

Im Folgenden wird die Erfindung anhand von Ausführungsbeispielen näher erläutert, die in den Figuren schematisch dargestellt sind. Gleiche Bezugsziffern in den einzelnen Figuren bezeichnen dabei gleiche Elemente. Im Einzelnen zeigt:

Fig. 1a, 1b und 1c zeigen eine symmetrische Verschlüsselung auf der Basis der Mod2-Operation, wobei ein Cypher die zufällige Crypto Sequenz erzeugt und eine Synchronisation auf der Basis des Anfangszustandes des Cyphers erfolgt;

Fig. 2a, 2b und 2c zeigen das Verfahren auf der Basis der vorliegenden Erfindung, wobei die Symbole aus dem Flash-Eprom verwendet werden, um eine Verschlüsselung durchzuführen; hierbei wird als Anfangszustand die Anfangsadresse übertragen, um dann schließlich diese Adresse voran zuschieben, so dass ein verbrauchter und ein unverbrauchter Bereich entstehen;

Fig. 3a und 3b zeigen das erfindungsgemäße Verfahren in einer alternativen Ausführungsform, wobei durch einen Pseudozufallsgenerator (PZG), dessen Zustand anfänglich übertragen wird, die Adresse bestimmt wird, aus der das Symbol vom Speichermedium Flash-Eprom zu lesen ist;

Fig. 4a und 4b zeigen Abwandlungen der Verfahren aus den Figuren 1 und 3, wobei in regelmäßigen Abständen Synchronisationsinformationen des Chyphers bzw. des PZGs übertragen werden;

Fig. 5 zeigt den Datenfluss bei einer bevorzugten Ausführungsform, die eine Verschlüsselung vornimmt;

Fig. 6 zeigt den Datenfluss bei einer bevorzugten Ausführungsform, die eine Entschlüsselung der in Figur 5 verschlüsselten Daten vornimmt.

Wie bereits in der Einleitung erwähnt, beschreiben die Figuren 1a bis 1c ein Verfahren, wie es aus dem Stand der Technik bekannt ist. Ein Chyper (Zufallsgenerator) erzeugt hierbei eine Sequenz, mit der die Daten durch eine Mod2-Operation verschlüsselt werden. Da der Chyper deterministisch ist, kann aufgrund des Zustandes die zukünftige Datenfolge bestimmt werden, wodurch eine Übertragung des Anfangszustandes möglich ist oder, wie aus Figur 4a ersichtlich ist, eine wiederholte Übertragung des Zustandes eine Synchronisation erlaubt.

Den Figuren 2a bis 2c ist die erfindungsgemäße Ausführungsform zu entnehmen. Hierbei werden die Symbole zur Verschlüsselung nicht durch einen Zufallsgenerator erzeugt, sondern liegen auf einem Speicher ab. Aufgrund der Größe der Flash-Speicher kann somit ein kompletter Datenstrom verschlüsselt werden. Anstatt des Zustandes des Chypers wird die Adresse auf dem Speichermedium übertragen.

Im Folgenden wird ein Beispiel zur Dauer der verschlüsselten Übertragungszeit in Abhängigkeit der FLASH-Größe aufgezeigt. Gegeben sei ein FLASH-EPROM der Größe $N_C = 2^{33} bit = 2GByte$. Für die Adressierung dieser Speichergröße werden $L_C = 33bit$ benötigt.

Angenommen eine digitalisierte Sprachinformation wird mit einer Datenrate $R_{VC} = 2400bit/s$ übertragen, wie es z. B. im GSM-Bereich oder im digitalen Funk der Fall ist, so kann bei

einmaligem Auslesen des gesamten FLASH-Inhaltes (OTP: one time pad), d. h. ohne Wiederverwendung einzelner Segmente, eine Gesamtdauer von

$$T_{OTP} = \frac{N_C}{R_{VC}} = 994.2 Stunden = 41.4 Tage$$

verschlüsselt übertragen werden. Da es sich hierbei um eine Netto-Zeit handelt, ist ein Speichermedium für die Verschlüsselung mehr als einen Monat bei sicherer Verschlüsselung einsetzbar. Erst dann sind die Speichermedien aller Beteiligten neu zu beschreiben bzw. zu initialisieren.

Die Figur 3 zeigt eine weitere Ausführungsform der vorliegenden Erfindung. Bei diesem Ansatz erzeugt ein Zufallsgenerator die Adresse für die Speicherkarte. Anstatt die Anfangsadresse der Karte oder die aktuelle Adresse (Figur 4b) zu übertragen, wird der Zustand des PZGs übertragen. Dadurch ist selbst im Falle des Verlustes einer Karte nicht unmittelbar ein Abhören möglich, da der Zufallsgenerator die Adressen nicht linear bestimmt. Für die Synchronisation wird, wie aus Figur 4b deutlich wird, immer wieder der Zustand des Zufallsgenerators übertragen.

Nimmt man an, dass ein Vocoder die zu übertragenden Symbole in Rahmen (Frames) der Dauer 20 ms zusammenfasst und dass die Datenrate des Vocoders $R_{VC} = 2000 bit/s$ sei, sodass in einem Rahmen ND=40 bit übertragen werden. Für die Übertragung der Synchronisationsinformation würden BS=14 bit zu Verfügung stehen. Hieraus ergibt sich, dass sich $N_S = 2^{B_S} = 16384$ Segmente der Crypto Sequenz mit einer Länge von je 40 bit adressieren lassen. Dies entspricht der Anzahl der Zustände des Pseudozufallsgenerators.

Die Figuren 5 und 6 zeigen eine weitere Ausführungsform der vorliegenden Erfindung. Zusätzlich zu den Permutationen der Informationen, bevor sie gesendet werden, wird ein zweiter

Zufallsgenerator (PZG1) eingesetzt. PZG1 dient zur Verwürfelung des Zugriffs auf einzelne Segmente der Crypto Sequenz, wenn PZG2 die konkreten Adressen o.g. Segmente bestimmt. Der Zustand des ersten Zufallsgenerators wird genauso im Crypto Text abgelegt wie die verschlüsselten Informationen, die mit den Symbolen an der Adresse des durch den PZG2 bestimmten Bereichs verschlüsselt wurden. Bei der Entschlüsselung wird der Zufallsgenerator anhand des übertragenen Zustandes synchronisiert, um dann das korrekte Segment von der bestimmten Adresse der Speicherkarte zu lesen, auf dessen Basis die Rücktransformation stattfindet. Anschließend wird die Permutation rückgängig gemacht.

Liste der zitierten Literatur:

[1] C. E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J. , vol. 27., Part1. pp. 379-423, Part 2. pp. 623-656, 1948.

[2] C. E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J., vol. 28., pp. 565-715, 1949.

[3] J. L. Massey, An introduction to contemporary cryptology, Proc. IEEE, vol. 76, pp. 533-549, May 1988.

Patentansprüche

1. Verfahren zur Verschlüsselung von digitalen Informationen,
- mit Kommunikationsgeräten, die eine Schnittstelle für ein austauschbares oder beschreibbares Speichermedium haben, dessen Inhalt auslesbar und duplizierbar ist,
- mit einem Speichermedium, das mit der Schnittstelle in Verbindung steht, wobei auf dem digitalen Speichermedium ein Vorrat an Symbolen zur Verschlüsselung abgelegt ist, der anhand einer Adresse auslesbar ist,
- mit einer Verschlüsselungseinheit, die den Vorrat an Symbolen für die Verschlüsselung und/oder Entschlüsselung des digitalen Datenstroms der Kommunikationsgeräte auf der Basis von mindestens einer Adresse verwendet.

2. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die Symbole auf dem Speichermedium nur einmalig verwendet werden und somit „aufgebraucht" werden.

3. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Symbole mit dem Datenstrom mit Mod2 verschlüsselt und entschlüsselt werden.

4. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass es sich bei dem mobilen Endgerät um ein Funkgerät, Laptop, PDA und/oder ein mobiles Telefon handelt, die eine Schnittstelle für eine

Speicherkarte aufweisen, die unempfindlich sind und in portablen Kommunikationsgeräten eingesetzt werden können.

5. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Speichermedium eine Flash-Speicherkarte, eine Festplatte und/oder eine optische Speicherplatte ist, deren Informationen adressierbar sind.

6. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass zur Synchronisation der Verschlüsselung die Adressen der zu verwendenden Symbole auf dem Speichermedium übertragen werden.

7. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass zur Synchronisation der Verschlüsselung die Adresse in bestimmten Abständen übertragen wird.

8. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass ein erster Zufallsgenerator (PZG2) auf dem Kommunikationsgerät vorhanden ist, der die Bestimmung der Adresse auf dem Speichermedium vornimmt.

9. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass zur Synchronisation der Verschlüsselung der Zustand des Zufallsgenerators übertragen wird.

10. Zustand des Zufallsgenerators übertragen wird.

11. Verfahren nach einem oder mehreren der Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass in bestimmten Abständen der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass ein zweiter Zufallsgenerator (PZG1) vorhanden ist, der eine Verwürfelung des Zugriffs auf einzelne Segmente vornimmt, wenn PZG2 die konkreten Adressen der Segmente bestimmt.

12. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass eine Permutation der digitalen Daten vorgenommen wird, bevor sie übertragen werden.

13. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Speichermedium durch das Rauschen einer analogen Quelle unter Verwendung eines A/D-Konverters beschrieben wird.

14. Kommunikationsgerät, das einen digitalen Datenstrom verschlüsselt,

- mit einer Schnittstelle für ein austauschbares oder beschreibbares Speichermedium, dessen Inhalt auslesbar und duplizierbar ist, wobei auf dem Speichermedium, das mit der Schnittstelle in Verbindung bringbar ist, ein Vorrat an Symbolen zur Verschlüsselung abgelegt ist, die durch Verwendung einer Adresse gelesen werden können,
- mit einer Verschlüsselungseinheit, die so eingerichtet ist, dass sie den Vorrat an Symbolen für die Verschlüsselung und/oder Entschlüsselung des digitalen Datenstroms der Kommunikationsgeräte

verwendet, indem durch Adressen auf diesen zugegriffen wird.

15. Kommunikationsgerät nach dem vorhergehenden Kommunikationsgeräteanspruch, gekennzeichnet durch eine Einrichtung, die die Symbole auf dem Speichermedium nur einmalig verwendet.

16. Kommunikationsgerät nach einem oder mehreren der vorhergehenden Kommunikationsgeräteansprüche, gekennzeichnet durch ein Rechenwerk, das die Symbole mit dem Datenstrom mit Mod2 verschlüsselt oder entschlüsselt.

17. Kommunikationsgerät nach einem oder mehreren der vorhergehenden Kommunikationsgeräteansprüche, dadurch gekennzeichnet, dass es sich um ein Funkgerät, Laptop, PDA und/oder ein mobiles Telefon handelt, die eine Schnittstelle für eine Speicherkarte aufweisen, wobei die Speicherkarte unempfindlich ist und in portablen Kommunikationsgeräten einsetzbar ist.

18. Kommunikationsgerät nach einem oder mehreren der vorhergehenden Kommunikationsgeräteansprüche, dadurch gekennzeichnet, dass das Speichermedium eine Flash-Speicherkarte, eine Festplatte und/oder eine optische Speicherplatte ist, deren Informationen adressierbar sind.

19. Kommunikationsgerät nach einem oder mehreren der vorhergehenden Kommunikationsgeräteansprüche, gekennzeichnet durch Mittel, die zur Synchronisation der Verschlüsselung die Adressen der zu verwendenden Symbole auf dem Speichermedium übertragen.

20. Kommunikationsgerät nach dem vorhergehenden Anspruch, gekennzeichnet durch Mittel, die zur Synchronisation der Verschlüsselung die Adresse in bestimmten Abständen übertragen.

21. Kommunikationsgerät nach einem oder mehreren der vorhergehenden Kommunikationsgeräteansprüche, dadurch gekennzeichnet, dass ein erster Zufallsgenerator (PZG2) auf dem Kommunikationsgerät vorhanden ist, der die Bestimmung der Adresse auf dem Speichermedium vornimmt.

22. Kommunikationsgerät nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass zur Synchronisation der Verschlüsselung der Zustand des Zufallsgenerators übertragen wird.

23. Kommunikationsgerät nach dem vorhergehenden Anspruch, gekennzeichnet durch Mittel, durch die in bestimmten Abständen der Zustand des Zufallsgenerators übertragen wird.

24. Kommunikationsgerät nach einem oder mehreren der vorhergehenden Kommunikationsgeräteansprüche, dadurch gekennzeichnet, dass ein zweiter Zufallsgenerator (PZG1) vorhanden ist, der eine Verwürfelung des Zugriffs auf einzelne Segmente vornimmt, wenn PZG2 die konkreten Adressen der Segmente bestimmt.

25. Kommunikationsgerät nach einem oder mehreren der vorhergehenden Kommunikationsgeräteansprüche, gekennzeichnet durch Mittel, die eine Permutation der digitalen Daten vornehmen, bevor die Daten übertragen werden.

26. Kommunikationsgerät nach einem oder mehreren der vorhergehenden Kommunikationsgeräteansprüche, dadurch gekennzeichnet, dass das Speichermedium durch das Rauschen einer analogen Quelle unter Verwendung eines A/D-Konverters beschrieben ist.

27. Verwendung eines mobilen adressierten Speicherelementes, wie einer Flash-Card, das durch ein mobiles Kommunikationsgerät lesbar ist, zur Ablage von Symbolen zur Verschlüsselung, wobei die Symbole adressierbar sind.

28. Software für ein Kommunikationsgerät, wie ein mobiles Endgerät, gekennzeichnet durch die Implementierung eines Verfahren nach einem oder mehreren der vorhergehenden Verfahrensansprüche.

29. Datenträger für einen Computer, gekennzeichnet durch die Speicherung einer Software nach dem vorhergehenden Softwareanspruch.

30. Computersystem mit einer Kommunikationsschnittstelle, gekennzeichnet durch eine Einrichtung, die den Ablauf eines Verfahrens nach einem oder mehreren der vorhergehenden Verfahrensansprüche erlaubt.

Verschlüsselungsverfahren

Zusammenfassung

Die Erfindung betrifft ein Verfahren zur Verschlüsselung von digitalen Informationen mit Kommunikationsgeräten, die eine Schnittstelle für ein austauschbares oder beschreibbares Speichermedium haben, dessen Inhalt auslesbar und duplizierbar ist, mit einem Speichermedium, das mit der Schnittstelle in Verbindung steht, wobei auf dem digitalen Speichermedium ein Vorrat an Symbolen zur Verschlüsselung abgelegt ist, der anhand einer Adresse auslesbar ist, mit einer Verschlüsselungseinheit, die den Vorrat an Symbolen für die Verschlüsselung und/oder Entschlüsselung des digitalen Datenstroms der Kommunikationsgeräte auf der Basis von mindestens einer Adresse verwendet.

(Fig. 5)

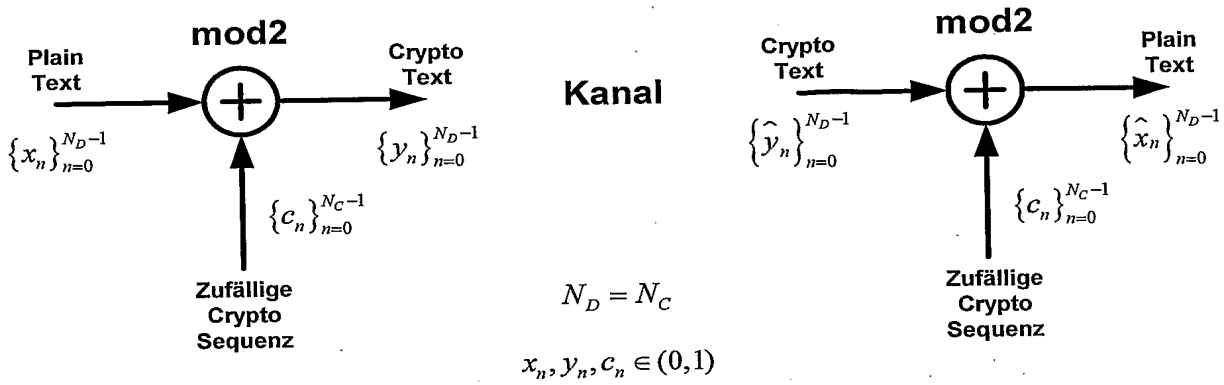

Fig. 1a (Stand der Technik)

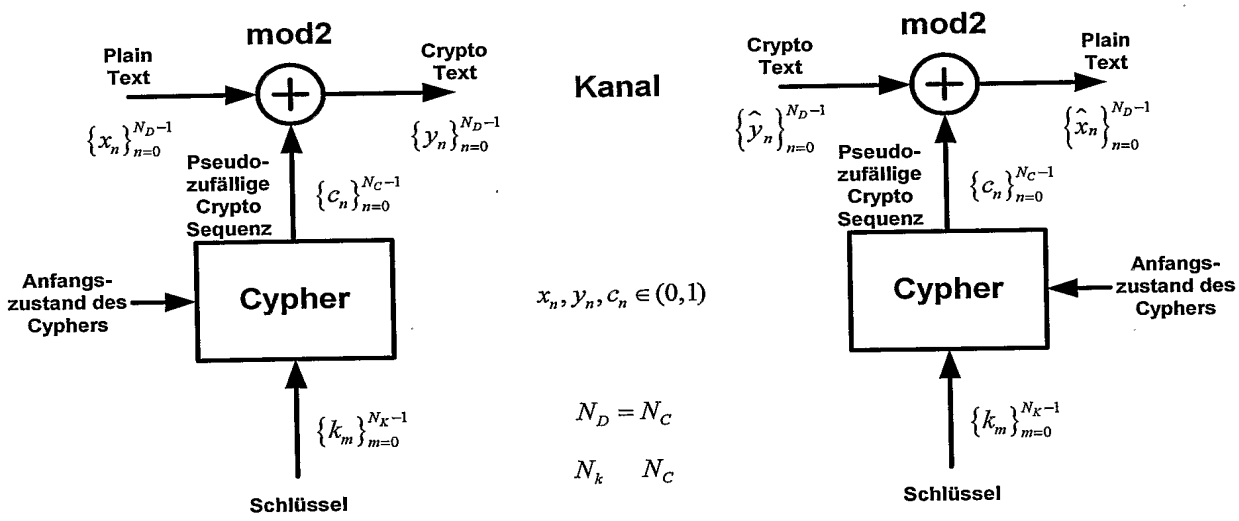

Fig. 1b (Stand der Technik)

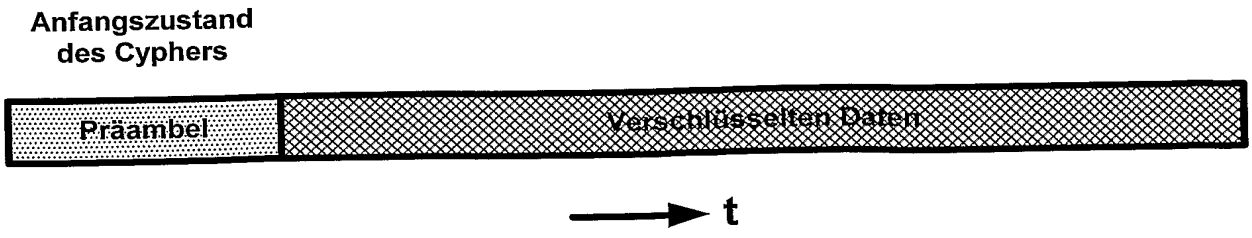

Fig. 1c (Stand der Technik)

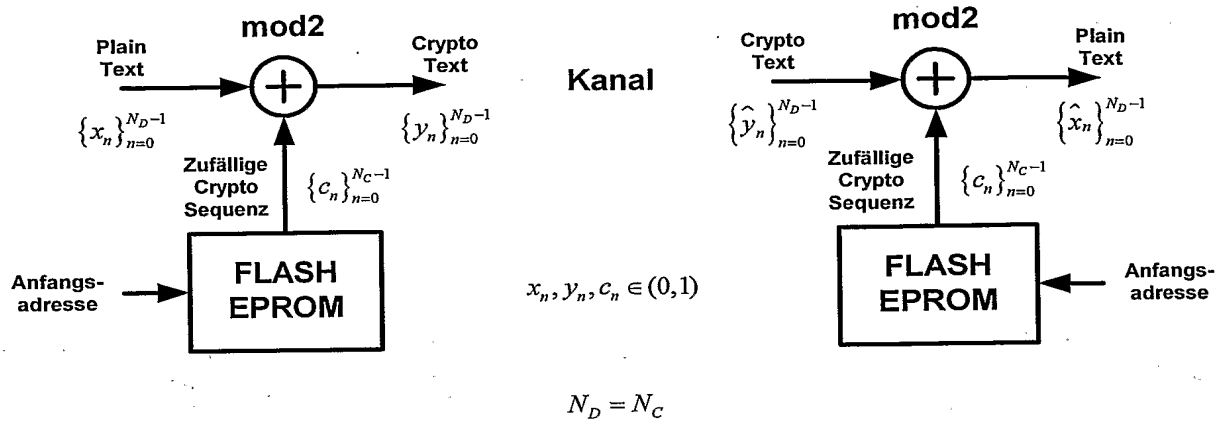

Fig. 2a

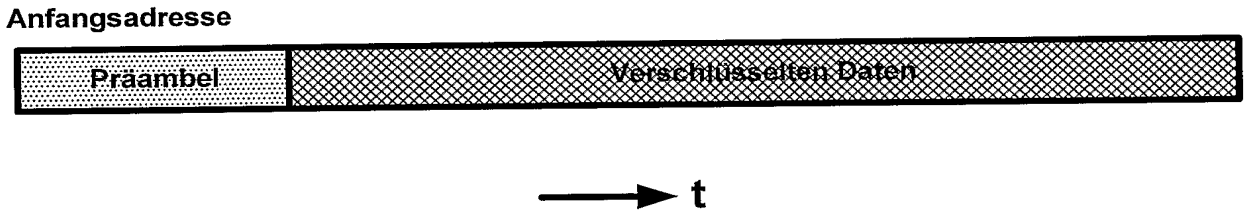

Fig. 2b

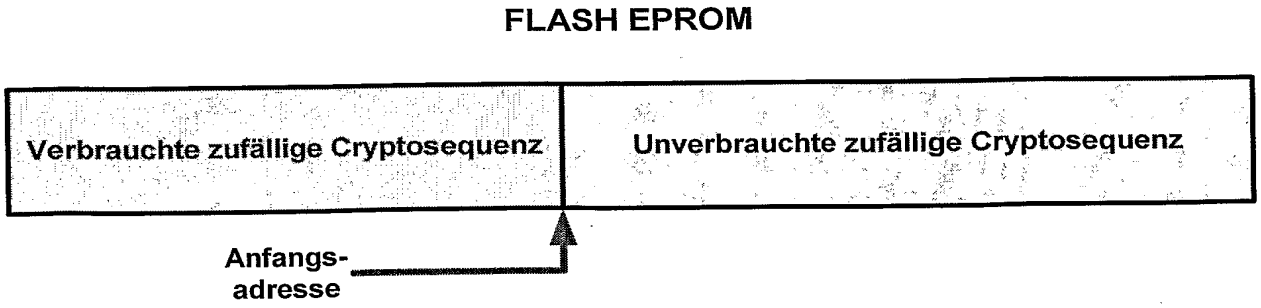

Fig. 2c

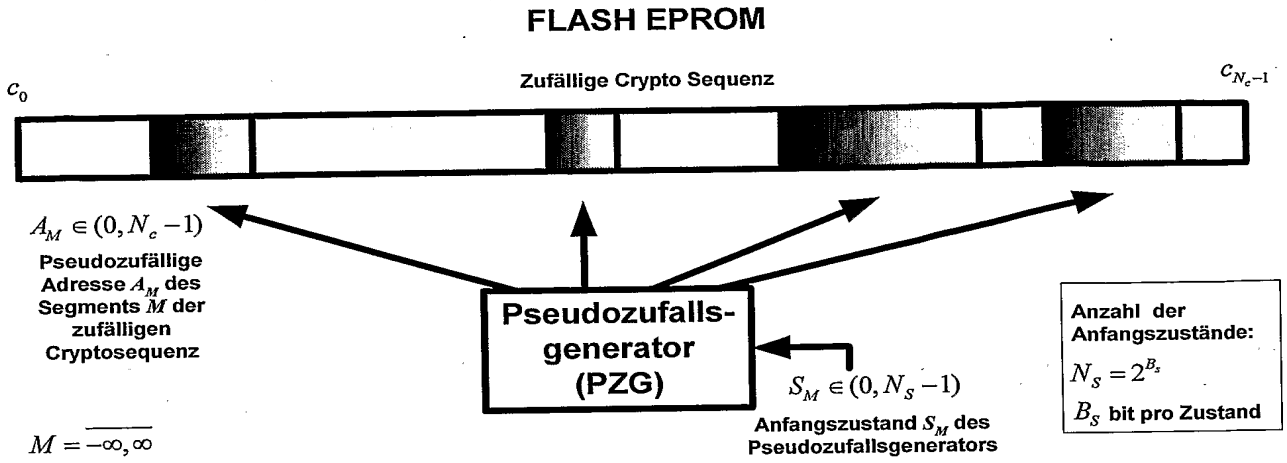
FLASH EPROM
Zufällige Crypto Sequenz
c_0
c_{N_c-1}
$A_M \in (0, N_c - 1)$
Pseudozufällige Adresse A_M des Segments M der zufälligen Cryptosequenz
$M = \overline{-\infty, \infty}$
Pseudozufalls-generator (PZG)
$S_M \in (0, N_S - 1)$
Anfangszustand S_M des Pseudozufallsgenerators
Anzahl der Anfangszustände:
$N_S = 2^{B_s}$
B_S bit pro Zustand

Fig. 3a

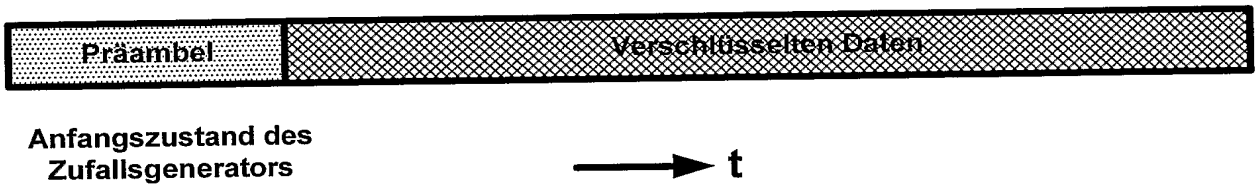
Präambel
Verschlüsselten Daten
Anfangszustand des Zufallsgenerators
t

Fig. 3b

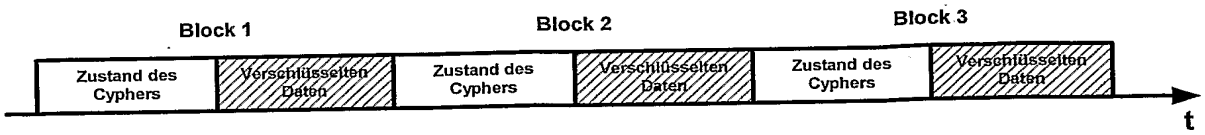

Fig. 4a (Stand der Technik)

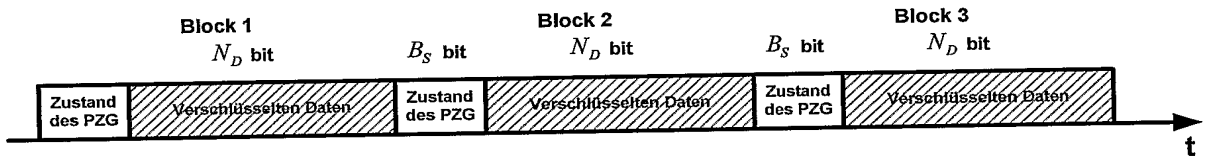

Fig. 4b

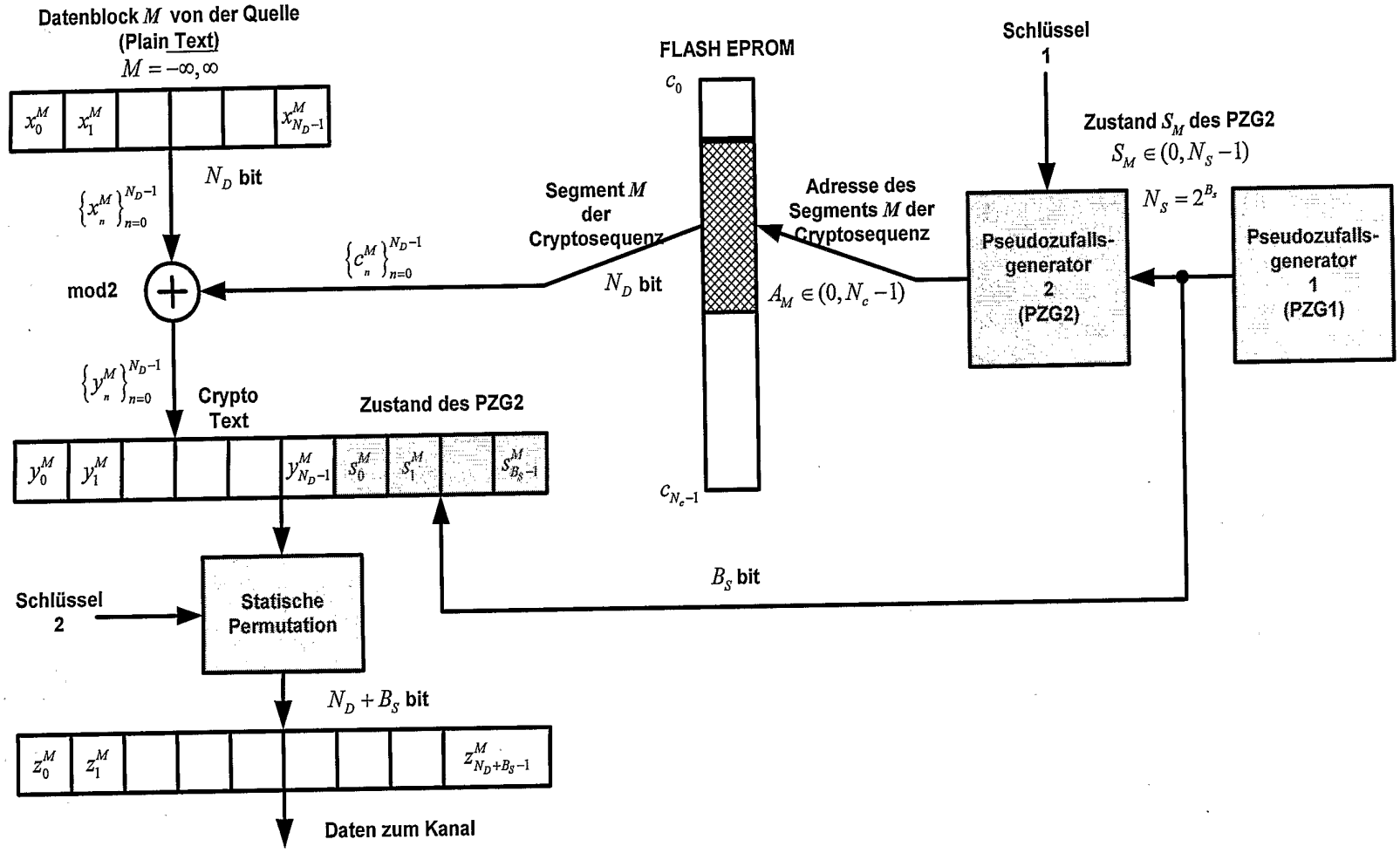
Datenblock M von der Quelle
(Plain Text)
$M = -\infty, \infty$
x_0^M x_1^M $x_{N_D-1}^M$
N_D bit
$\{x_n^M\}_{n=0}^{N_D-1}$
mod2
$\{c_n^M\}_{n=0}^{N_D-1}$
N_D bit
Segment M der Cryptosequenz
FLASH EPROM
c_0
c_{N_c-1}
Adresse des Segments M der Cryptosequenz
$A_M \in (0, N_c - 1)$
Schlüssel 1
Zustand S_M des PZG2
$S_M \in (0, N_S - 1)$
$N_S = 2^{B_S}$
Pseudozufalls-generator 2 (PZG2)
Pseudozufalls-generator 1 (PZG1)
$\{y_n^M\}_{n=0}^{N_D-1}$
Crypto Text
Zustand des PZG2
y_0^M y_1^M $y_{N_D-1}^M$ s_0^M s_1^M $s_{B_S-1}^M$
B_S bit
Schlüssel 2
Statische Permutation
$N_D + B_S$ bit
z_0^M z_1^M $z_{N_D+B_S-1}^M$
Daten zum Kanal

Fig. 5

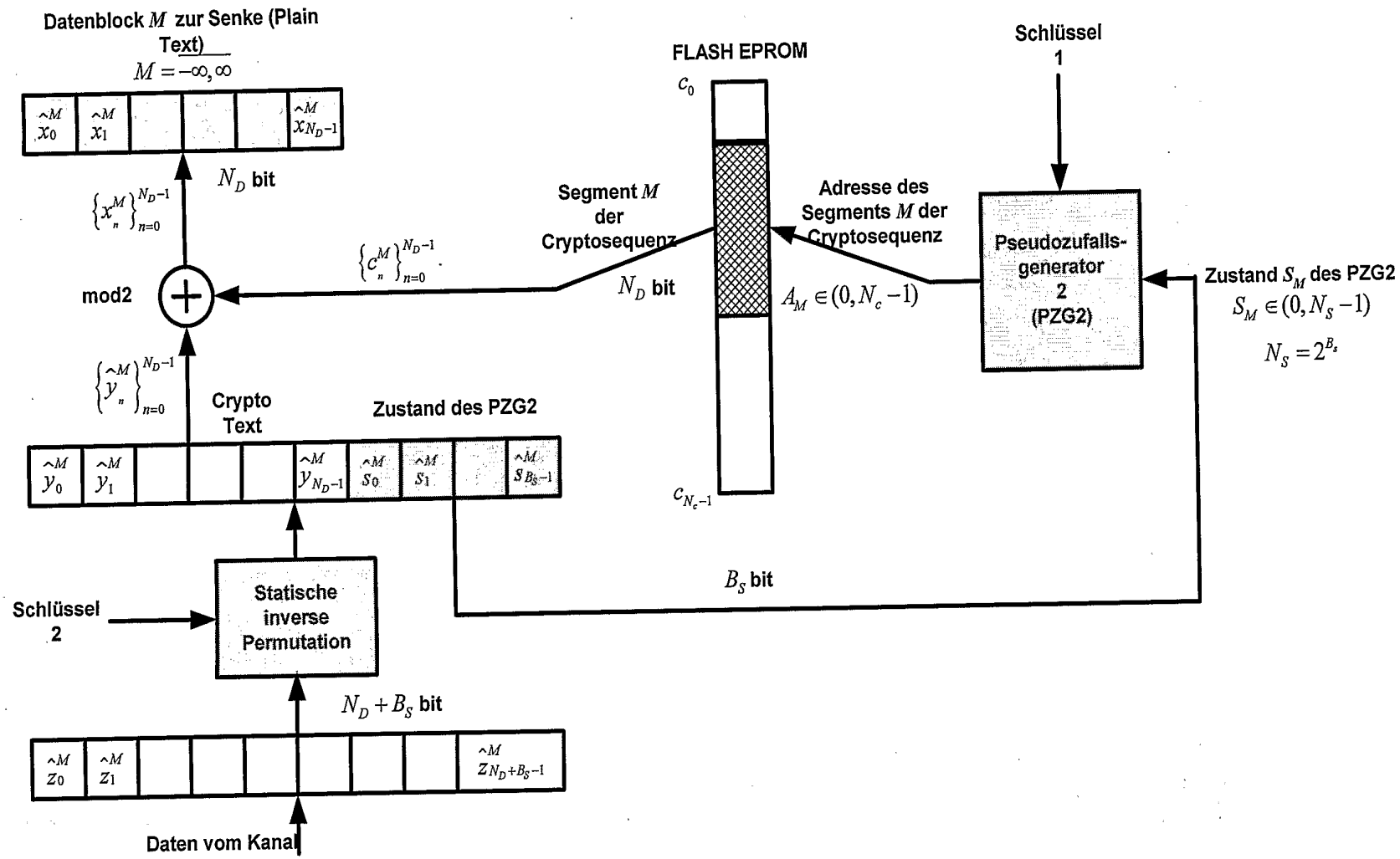
Datenblock M zur Senke (Plain Text)
$M = -\infty, \infty$
N_D bit
$\{x_n^M\}_{n=0}^{N_D-1}$
mod2
$\{c_n^M\}_{n=0}^{N_D-1}$
Segment M der Cryptosequenz
N_D bit
FLASH EPROM
c_0
c_{N_c-1}
Adresse des Segments M der Cryptosequenz
$A_M \in (0, N_c - 1)$
Schlüssel 1
Pseudozufalls-generator 2 (PZG2)
Zustand S_M des PZG2
$S_M \in (0, N_S - 1)$
$N_S = 2^{B_S}$
$\{y_n^M\}_{n=0}^{N_D-1}$
Crypto Text
Zustand des PZG2
B_S bit
Schlüssel 2
Statische inverse Permutation
$N_D + B_S$ bit
Daten vom Kanal

Fig. 6